

Remarks

Reconsideration of this Application is respectfully requested.

Upon entry of the foregoing amendment, claims 1, 3, 5, 6, 9-15, 17, 19, 20, 23-28, and 41-50 are pending in the application, with claims 1 and 15 being the independent claims. Claims 2, 4, 8, 16, 18, and 22 are sought to be cancelled without prejudice to or disclaimer of the subject matter therein. Claims 7, 21, and 29-40 were previously canceled. Claims 1, 15, and 20 are sought to be amended. New claims 41-50 are sought to be added. These changes are believed to introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and the following remarks, Applicants respectfully request that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Rejections under 35 U.S.C. § 112

Claims 1-6, 8-20, and 22-28 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicants respectfully traverse this rejection.

Claims 1 and 15 have been amended to remove the language cited by the Examiner in the rejection. Claims 2, 4, 16, and 18 have been canceled by the above amendment. Reconsideration and withdrawal of this rejection is therefore respectfully requested.

Rejections under 35 U.S.C. § 103

Kanda, Callum, Mano, Bianco

In the Office Action, claims 1-6, 8-20, and 22-28 were rejected under 35 U.S.C. §103(a) as being unpatentable over Kanda, et al, U.S. Patent No. 6,769,063 (Kanda) in view of Windirsch, U.S. Patent No. 6,760,439 (Windirsch), and further in view of Callum, U.S. Patent No. 6,320,964 (Callum). Applicants respectfully traverse this rejection.

The combination of Kanda, Windirsch, and Callum does not teach or suggest each and every element of Applicants' amended claims 1 and 15. Specifically, the combination does not teach or suggest:

two-level multiplexer circuitry including

a first level having a first 2-1 multiplexer and a second 2-1 multiplexer, wherein the first 2-1 multiplexer receives the left portion of the initial input data bit sequence at a first input and a right portion of the input bit sequence for a previous cryptographic round at a second input and wherein the second 2-1 multiplexer receives the right portion of the initial input data bit sequence at a first input and the right portion of the input bit sequence for the previous cryptographic round at a second input, and

a second level having a third 2-1 multiplexer and a fourth 2-1 multiplexer, wherein the third 2-1 multiplexer receives the output of the first 2-1 multiplexer at a first input and a right portion of an output bit sequence for a previous cryptographic round at a second input and wherein the fourth 2-1 multiplexer receives the output of the second 2-1 multiplexer at a first input and a right portion of the output bit sequence for the previous cryptographic round at a second input; ...

wherein the two-level multiplexer is configured to swap the left portion of the output bit sequence of a previous cryptographic round with the right portion of the output bit sequence of the previous cryptographic round

The benefit of the two level multiplexer, as recited in amended independent claims 1 and 15, is that the timing critical right portion of the output bit sequence of the previous cryptographic round is arranged to go through only the second level of the multiplexer. (See Specification, paragraph [0042]). The combination of Kanda, Windirsch, and Callum does not teach or suggest, at least, this recitation.

For at least these reasons, amended independent claims 1 and 15 are patentable over the combination of Kanda, Windirsch, and Callum. Claims 3, 5, 6, and 9-14 depend from claim 1. Claims 17, 19, 20, and 23-28 depend from claim 15. For at least these reasons, and further in view of their own features, claims 3, 5, 6, 9-14, 17, 19, 20, and 23-28 are patentable over the combination of Kanda, Windirsch, and Callum. Reconsideration and withdrawal of this rejection is therefore respectfully requested.

Kanda, Callum, Mano, Bianco

In the Office Action, claims 4 and 18 were rejected under 35 U.S.C. §103(a) as being unpatentable over Kanda in view of Windirsch and further in view of Callum and Steinman, et al., U.S. Patent No. 6,591,349. Claims 4 and 18 have been canceled by the above amendment, rendering this rejection moot.

New Claims

Applicants have added new claims 41-50. Applicants submit that claims 41-50 are patentable over the cited art. Accordingly, Applicants respectfully requests prompt indication of their allowance.

Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicants therefore respectfully request that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicants believe that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.



Lori A. Gordon
Attorney for Applicants
Registration No. 50,633

Date: May 30, 2006

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

537897_1.DOC